**INTRODUCTION**

Risk-based security (RBS) is a trend currently brought up often in numerous research and development programs across the globe, especially in the context of border crossing, where traveler satisfaction and experience are put to the test in long security lines and annoying checks, pat-downs, or the occasional hands-up posing on backscatter X-ray machines. The airport security checkpoint collects and deploys the latest and most efficient tactics in security border control procedures, given the actual but also emblematic role of the airplane as a transland and transocean mode of transport for millions of passengers. Given the impact connected to a highly prestigious target, what seems annoying for some passengers is also widely accepted by the vast majority as necessary and even comforting just to know it is there.

In this security context, RBS states a seemingly attractive case where security can be focused on fewer people in an intelligent way instead of “harassing” the vast majority of harmless passengers and travelers. Following the U.S. Department of Homeland Security’s Transportation Security Administration’s much criticized behavior and personality analysis programs, RBS and behavior analysis have now become a much more mainstream research topic and are handled through numerous initiatives. Part of the International Air Transport Association/Airports Council International (IATA/ACI) former Checkpoint of the Future recommendations— now Smart Security—RBS in airport security checkpoints is the main topic of research for the ongoing H2020 FLYSEC project, which is funded by the European Commission.

With apparent benefits to the efficiency and performance of security controls, RBS is equally sullied, if not overshadowed, by the concerns and threats to privacy, ethics, and fundamental values. Differentiating one passenger from another can be immediately followed by the frustration of the person being in the worst side of the “bargain.” If discrimination is imposed, e.g., based on race, gender, or religious beliefs, then aviation security will have to face costs in terms of ethics and human values that will also be translated to financial losses given the poor passenger experience, not to mention potential lawsuits. In fact, the emotional impact and cost of people feeling discriminated against are both so high that RBS not only has to be fair and ethical but also perceived as such to passengers.

In this article, we investigate the potentials of automated security decision making in terms of operational and technological opportunities, evaluating the threats and implications according to the latest privacy and ethical framework, given also the recent GDPR release.

In particular, we focus on data mining and machine-learning applications and relevant risks, also proposing an expert system capable of analyzing fairness and detecting deviations that might potentially lead to discrimination and violations of human rights.

**RBS Concept**

RBS is, in fact, not a new practice. Human operators and screeners at border control have always been practicing RBS. Many attacks have been avoided in the past due to training and experience as well as the gut feeling of security personnel who just spotted someone behaving oddly amid the crowd. However, with the latest intelligent surveillance and analytics technology developments, RBS comes into the picture as an innovative end-to-end operational and technical framework. Through advancements in AI and mainly through the application of machine learning, security professionals have greatly augmented their capability of analyzing data concerning the behavior and profile patterns of attackers, both in terms of volume of data and availability of sources, including a wide range of national and international law enforcement authorities’ data bases , passenger name records (PNR), and open source web intelligence to name a few.